Listing of the Claims:

The following is a complete listing of all the claims in the application, with an indication of the status of each:

Claim 1 (Previously Presented). A method for selectively denying access to encoded data, said method comprising the steps of:

loading an encryption key into a mission planning workstation at a first location;

connecting a media device to said mission planning workstation;

loading said encryption key from said mission planning workstation into said media device;

encrypting sensitive data using said encryption key;

loading the encrypted data onto the media device;

loading unencrypted data onto a media device, wherein data necessary to enable a target portable computing device associated with a vehicle to return to a location selected as a mission end location remains unencrypted;

disconnecting said media device from the mission planning workstation;

connecting a media device to the target portable computing device;

powering up the target portable computing device, thereby enabling it to execute a desired program or process;

transferring said encryption key to volatile memory from said media device;

transporting the target portable computing device and media devices to a location physically distant from the mission planning workstation;

deleting said encryption key from said media device in response to said transport step;

maintaining said encryption key only in volatile memory after said deleting step; and

deleting the encryption key from volatile memory resident on the target portable computing device responsive to an operator; or

automatically deleting the encryption key from volatile memory resident on the target portable computing device in the event of a loss of power to the target portable computing device.

2 (Canceled).

3 (Previously Presented). A method as recited in claim 1, wherein the step of deleting the encryption key responsive to an operator overwrites the location in non-volatile memory where the encryption key previously resided a desired number of times.

4 (Previously Presented). A method as recited in claim 1, wherein the step of deleting is triggered by an indication that a vehicle used for transporting the target portable computing device has left a home base.

5 (Currently Amended). A method as recited in claim 1, wherein the step of encrypting sensitive data further comprises the steps of:

selecting an encryption key, wherein the encryption key comprises a number of bits sufficient to prohibit an unauthorized person from "breaking" the encryption key at a desired level of difficulty~~; and~~.

6 (Original). A method as recited in claim 5, wherein an operator of the target portable computing device has no knowledge of the encryption key used to encrypt data on the at least one media device in the encrypting step, and the encryption key is maintained at the home base mission planning workstation.

7 (Original). A method as recited in claim 5, wherein the step of selecting an encryption key selects a new key on a desired periodic basis, thereby minimizing a risk of compromise of a previously used encryption key.

8 (Previously Presented). A method as recited in claim 1, wherein said deleting step responsive to an operator is performed upon perceiving a threat by a member of the mission.

9 (Original). A method as recited in claim 8, further comprising the step of transporting the vehicle to the selected mission end location, wherein encrypted data remains encrypted and unencrypted data enables the vehicle to operate at with sufficient performance to arrive at the mission end location.

10 (Canceled).

11 (Currently Amended). A method as recited in claim ~~10~~ 1, further comprising the step of transporting the vehicle to the selected mission end location, wherein encrypted data remains encrypted and unencrypted data enables the vehicle to operate at with sufficient performance to arrive at the mission end location.

12 (Previously Presented). A system for selectively denying access to encoded data, comprising:

a selected encryption key, the key being of a number of bits sufficient to deter compromise of sensitive data to a desired difficulty level;

a target portable computing device loaded onto a land, sea, air or space vehicle, the target portable computing device used for mission specific tasks and having connections for at least one media device, wherein sensitive encrypted data and/or unencrypted benign data is to be loaded on the at least one media device depending on mission parameters, the target computing device comprising:

means to delete the encryption key from volatile memory resident on the target portable computing device in the event of a threat, whether perceived or real responsive to an operator; and

means to automatically delete the encryption key from volatile memory resident on the target portable computing device in the event of a loss of power to the target portable computing device;

a mission planning workstation connected to at least one media device during loading and encryption of sensitive data, and loading of unencrypted benign data, wherein the encryption key is loaded into the at least one media device and erased from said at least one media device after commencement of the mission,

wherein after sensitive data is encrypted on at least one media device connected to the mission planning workstation, each of the at least one media devices are connected to the target portable computing device and the encryption key is resident only in volatile memory on any media device connected to the target portable computing device after mission commencement, and

wherein sufficient unencrypted data resides on at least one media device connected to the target portable computing device to enable the mission vehicle to return to a selected mission end location in the event that the encryption key is deleted from volatile memory on the target portable computing device during the mission.

13 (Previously Presented). A system as recited in claim 12, further comprising:

means for communication between the mission planning computer and at least one media device and target portable computing device, wherein the at least one media device is connected simultaneously to both the mission planning workstation and the target portable computing device prior to mission commencement and during data encryption.